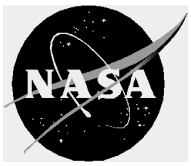
National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
2101 NASA Road 1
Houston, Texas 77058-3696



Reply to Attn of : MA2-00-057

September 28, 2000

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration
OA/Deputy Manager, International Space Station Program

SUBJECT: Mechanical Systems Safety

The information contained in this letter is an interpretation and clarification of the payload safety requirements for the Space Shuttle Program (SSP) and for the International Space Station (ISS) Program. This letter applies to all SSP and ISS Program payloads; i.e., payloads required to comply with either NSTS 1700.7B paragraph 200.2, “Safety Policy and Requirements for Payloads Using the Space Transportation System” or NSTS 1700.7B, ISS Addendum paragraph 200.2, “Safety Policy and Requirements for Payloads Using the ISS.” This letter will be utilized by the flight Payload Safety Review Panel (PSRP) in assessing safety compliance. This letter replaces the previous letter, TA-94-041, “Mechanical Systems Safety,” dated June 9, 1994. Please add this letter to your copy of NSTS/ISS 18798B, "Interpretations of NSTS/ISS Payload Safety Requirements," as applicable against NSTS 1700.7B and the ISS Addendum. Enclosed is an updated table of contents for NSTS/ISS 18798B.

This letter is intended to consolidate and clarify the major PSRP policy decisions on matters related to the safety requirements for the design and verification of mechanisms (movable mechanical systems) used in safety critical applications. This letter addresses assurance of safety critical functionality (the ability to operate or the ability to retain configuration) for mechanical systems rather than their strength as a structural element or the electrical aspects of an electromechanical system. For the purposes of this letter, safety critical refers to a system which has the potential to result in a critical or catastrophic hazard.

The revised safety policy, as documented in this letter, provides clarification on usage of the design for minimum risk (DFMR) approach as it applies to functionality of a movable mechanical system. This revised safety policy specifies that compliance with DFMR criteria when applied to movable mechanical systems normally can be used to establish safety compliance in designs with only one additional control or backup for a catastrophic hazard or without additional controls for a critical level hazard. Additionally, this revised safety policy also permits the use of fully compliant simple mechanical systems without mechanical redundancy, i.e., DFMR simple mechanisms can be considered as having two-failure-tolerance equivalency when specifically approved by the PSRP.

A simple mechanical system is defined as a robust mechanism that has relatively few moving parts and can demonstrate low sensitivity to environmental and operational conditions. If a hardware developer elects to follow the simple mechanical system route,

approval must be obtained from the PSRP prior to completion of the phase I safety review. The Mechanical Systems Working Group (MSWG) will support this process by assessing the level of assurance that all credible hazardous failure modes have been identified and that each of these failures will be reliably and effectively controlled as a result of a thorough design, build, and test process.

The design of a movable mechanical system can be considered to meet DFMR in functionality if it can be demonstrated that credible failure modes have been reliably and effectively controlled as a result of a thorough design, build, and test process. Failure modes that must be considered for credibility include, but are not limited to, binding, jamming, inadvertent operation, failure to function, etc. The DFMR approach must include design implementation and verification provisions outlined in items 1 through 11 of this letter, unless clearly not applicable, to enhance the safety critical reliability of mechanical systems to the maximum extent practical. These items will be topics of the review process for all safety critical mechanical systems. The PSRP may accept alternate approaches to the design, build, and test provisions contained herein on a clearly substantiated equivalent safety basis with the MSWG's recommendation.

1.0 Binding/Jamming/Seizing. Designs shall include provisions to prevent binding/jamming/seizing. Appropriate design provisions include, but are not limited to, dual rotating surfaces or other mechanical redundancies, robust strength margins such that self-generated internal particles are precluded, shrouding and debris shielding, proper selection of materials and lubrication design to prevent friction welding or galling, etc. Designs shall also establish dimensional tolerances on all moving parts to ensure that proper functional performance will be maintained under all natural and induced environmental conditions including, but not limited to, thermally induced in-plane and out-of-plane distortions, differential thermal growth and shrinkage, and load-induced deflections. The design shall also take into account tolerances associated with rigging (mechanical adjustment) and shall demonstrate by test and/or analysis that the sensitivity of mechanism performance as a function of rigging tolerances or installation/integration variables is understood. Additionally, mechanical system designs shall ensure compatibility of any lubricants used with interfacing materials and other lubricants used in the design, and shall ensure the lubrication is compatible with the natural and induced environment. The design shall also address proper quantities of lubricant.

2.0 Quick Release Pins. Quick release pins (pip-pins) used in safety critical applications are considered movable mechanical systems subject to the provisions of this letter. A pip-pin design qualified by inspection and test to the provisions of MIL-P-23460 or equivalent shall be used in any system design incorporating safety critical pip-pins. Flight pip-pins shall be subjected to environmental acceptance testing. Pip-pins shall be vibration tested to qualification levels in place in their respective hardware locations during the qualification test of the total assembly, or they may be tested alone in a component test to the predicted qualification levels at the hardware location. Pip-pins shall also be subjected to thermal testing to the maximum/minimum qualification temperatures. Due to a history of failures with pip-pins, the simple mechanical system approach identified above is not applicable.

3.0 Springs. In designs and applications where spring failure would result in a hazard, the springs shall be redundant or designed, evaluated, and used under an acceptable fracture control program (reference NASA-STD-5003). Failure of springs that are properly

controlled under an acceptable fracture control program, is considered noncredible. The design and use of a fail-safe spring or the use of a spring that maintains functionality with the loss of a single coil is acceptable. Where practical, compression springs should be used in lieu of tension or torsional springs.

4.0 Fastener Retention. A means of positive locking (i.e., self-locking threads, self-locking inserts, etc.) shall be provided on all fasteners (threaded and otherwise) to assure integrity of the mechanical assemblies and prevent loose parts. This is in addition to the standard torque/preload of the fastener. Where other locking devices are practicable, locking compounds shall not be used on fasteners to provide locking.

5.0 Strength and Fracture Control. Structural design of safety critical mechanical system components shall adhere to paragraphs 208.1, 208.2, and 208.3 of NSTS 1700.7. Movable mechanical assemblies used in safety critical applications shall be included in an acceptable fracture control program (reference NASA-STD-5003). Mechanical system components and linkages shall be designed with sufficient strength to tolerate an actuation force/torque stall condition at any point of travel and maintain a positive margin of safety with an ultimate factor of safety applied. Mechanical systems that incorporate end of travel mechanical stops shall be designed to have positive strength margins for worst case dynamic loading conditions, considering variables in inertia properties, actuation force/torque, drive train resistance, and other environmental conditions. Exposed mechanical system components, protective shrouds and covers, and mounting structure shall be designed to accommodate inadvertent impact loads from remote manipulator system/ISS remote manipulator system/payload operations and extravehicular activity/intravehcular activity loads, as appropriate, to ensure adequate margins to preclude deformation that could cause a binding or jamming condition or inadvertent operation of the mechanism. A design that incorporates preload as a means of meeting functional and/or structural requirements shall comply with the preload criteria defined in NSTS 08307.

6.0 Positive Indication of Status. All movable mechanical systems shall provide positive indication that the mechanism has achieved its desired position (i.e., ready-to-latch, latched). End of travel stops shall be provided for all movable mechanical systems.

7.0 Torque/Force Margins. For movable mechanical systems in safety critical applications, the operating torque or force margin shall be acceptance-test verified unless another verification approach is approved by the MSWG. When test verified, a margin of 1.0 or greater is required at applicable points of travel. Verification by analysis only will require prior review and approval of the analytical approach and margin requirement by the MSWG. This margin, as demonstrated conservatively by test or analytical calculations, shall take into account worst case environmental conditions, frictional effects, alignment effects, latching forces, thermally induced distortions, load induced distortions, and variations in lubricity including degradation or depletion of lubrication under vacuum and under worst case thermal conditions, etc. Operating torque margin is defined as:

$$\textit{Operating Torque Margin} = \textit{(Available Driving Torque / Resisting Torque)} - 1$$

For linear devices, “Force” replaces “Torque” in the above equation.

Mechanism holding torque or force margin shall be acceptance-test verified unless another verification approach is approved by the MSWG. When test verified, a margin of 1.0 or greater is required in the applicable mechanism holding configuration(s). The holding torque or force margin is the margin provided to prevent inadvertent operation. Verification by analysis only will require prior review and approval of the analytical approach and margin requirement by the MSWG. This margin, as conservatively demonstrated by test or analytical calculations, shall take into account worst case environmental conditions, frictional effects, alignment effects, latching forces, thermally induced distortions, and load induced distortions, etc. The holding torque margin is defined as:

Holding Torque Margin = (Available Holding Torque / Torque Applied by Limit Load) - 1

For linear devices, “Force” replaces “Torque” in the above equation.

Verification by test, as specified in this paragraph, does not require a mechanical system demonstration at greater than limit load conditions but rather requires a test verification of the amount of driving or holding torque or force available under conservative adverse conditions.

8.0 Contamination. Fabrication and handling of safety critical movable mechanical assemblies shall be accomplished in a clean environment with attention given to avoiding nonparticulate (chemical) as well as particulate air contamination. Specific cleanliness requirements shall be established for each movable mechanical assembly and shall address cleanliness levels needed to prevent binding or jamming.

9.0 Assembly Level Acceptance Tests. Each movable mechanical assembly designated for flight or as a qualification test article shall be subjected to acceptance testing which incorporates run-in, functional, and environmental testing. The acceptance tests shall be structured to detect workmanship defects that could affect operational performance. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion.

9.1 Run-in Test. After initial functional testing, a run-in test shall be performed on each movable mechanical assembly before it is subjected to further acceptance testing. The purpose of the run-in test is to detect material/workmanship defects and to wear-in parts.

9.2 Functional and Environmental Acceptance Tests. Each movable mechanical assembly shall be subjected to functional and environmental tests. Functional tests shall be structured to demonstrate that the movable mechanical assembly is capable of operating to satisfy all performance requirements. Functional tests are required before and after exposure to environmental test conditions in order to establish whether damage or degradation in performance has occurred. Environmental acceptance tests shall be structured to demonstrate the ability to achieve performance requirements when exposed to the expected environmental extremes and to identify any workmanship defects.

10.0 Qualification Test. A Qualification Test Program shall be established for each safety critical movable mechanical assembly. The qualification test program shall assure that a design performance and safety margin exists with respect to all design requirements when exposed to any mechanical, electrical, environmental, including acceptance testing, and

operational stimuli that the product may reasonably expect to encounter during its service life. The mechanism shall be tested in its launch, on-orbit, and landing configurations with the appropriate corresponding environmental extremes and with the mechanism in its appropriate passive or operating state. Inspection and functional tests are required before and after qualification tests. MIL-STD-1540D may be helpful in establishing an effective Qualification Test Program. Natural and induced environmental conditions shall include but are not limited to, thermally induced in-plane and out-of-plane distortions, differential thermal growth and shrinkage, and load-induced deflections. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion.

11.0 Design Life Verification Tests. For applications where design life might be a concern due to endurance or fatigue limits being exceeded, potential deterioration of lubrication, or excessive wear, design life verification testing shall be conducted to verify that design life requirements have been complied with. Design life testing for mechanisms that pose a catastrophic hazard potential shall assure at least four times the number of operational cycles, plus four times the number of component and vehicle functional and environmental test cycles. Design life testing for mechanisms that pose a critical hazard potential shall assure at least two times the number of operational cycles, plus two times the number of component and vehicle functional and environmental test cycles. Inspection and functional tests are required before and after design life verification tests. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion. Refurbishment shall be accomplished after the design life verification tests and prior to reacceptance testing.

A comprehensive Mechanical Systems Verification Plan that describes the verification approach for safety critical movable mechanical systems must be submitted for review and approval by the MSWG. The specific purpose of this plan is to establish an understanding on how applicable systems requirements will be implemented and verified. Before a movable mechanical system can be classified as a DFMR Mechanical System, compliance to the subject letter requirements must be provided to and approved by the MSWG. Although cancelled, mechanical system designers may still refer to MIL-A-83577 as a guideline during the design and verification process. Questions concerning this letter should be directed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, JSC/NC4, at (281) 483-8848.

Original Signed By: ***Original Signed By:***

William H. Gerstenmaier Jay H. Greene

Enclosure

cc:
See List

Distribution:
CB/G. D. Griffith
DO12/J. M. Childress
EA44/R. J. Wren
MA2/A. M. Larsen
MA2/D. E. O'Brien
MA2/D. W. Whittle
MA2/J. G. Williams
NC4/M. L. Ciancone
NC55/SAIC/E. J. Conner
NE2/G. L. Priest
OZ3/D. W. Hartman
SD2/M. E. Coleman
USA/USH-700D/H. A. Maltby

cc:
AE/J. F. Whiteley
CA/J. D. Wetherbee
CB/C. J. Precourt
DA/B. R. Stone
EA/L. S. Nicholson
EA4/D. A. Hamilton
KN/NASDA/T. Akutsu
LM/I. M. Dornell
MA/R. D. Dittemore
MG/R. H. Heselmeyer
MM/J. B. Costello
MM/T. W. Logan
MQ/M. D. Erminger
MS/L. D. Austin, Jr.
MS3/D. L. Ladrach
MS3/K. B. Packard
MT/R. M. Swalin
MV/R. R. Roe, Jr.
NC44/M. L. Mudd
OA/T. W. Holloway
OE/J. B. Holsomback
OI/W. J. Bennett
OR/CSA/H. L. Williams
OT/ESA/U. J. Thomas
XA/G. J. Harbaugh
HQ/M-4/W. M. Hawes
HQ/MO/S. R. Nichols
HQ/M-7/N. B. Starkey
KSC/EC-G1/J. C. Dollberg
KSC/MK/J. D. Halsell, Jr.
KSC/MK-SIO/R. L. Segert
USA/USH-700D/L. Lo

Canadian Space Agency
Space Station Program
Attn: P. M. Jean
Manager, Safety and Product Assurance
6767 route de l'Aeroport
Saint-Hebert, Quebec
Canada J3Y 8Y9

ESTEC-GPQ
Attn: T. Sgobba
T. Heimann
P. O. Box 299 NL
2200 AG, Noordwijk
The Netherlands

NASDA
Tsukuba Space Center
Attn: H. Hasegawa
Space Station Safety and Product
Assurance Office
Reliability Assurance
2-1-1 Sengen
Tsukuba-shi, Ibaraki
Japan 305

RSC Energia
Attn: P. Vorobiev
4a Lenin Street
Korolev
141070 Moscow Region
Russia